REMARKS

By this amendment, claims 1-21 are pending, in which no claims are canceled, withdrawn from consideration, amended, or newly presented. No new matter is introduced.

The Office Action mailed March 24, 2004 rejected claims 1-21 under 35 U.S.C. § 103(a) as obvious over *Liu* (U.S. 6,079,020) in view of *Tabata* (U.S. 2001/0016914).

The obviousness rejection of claims 1-21 is respectfully traversed, as the applied art does not disclose or suggest preventing or resisting denial of service attacks.

For example, independent claim 1 recites "a network system that **resists denial of service attacks on an access link to a destination host belonging to a virtual private network (VPN)**, said network system comprising: one or more egress boundary routers having connections to an access network including the access link, wherein said one or more egress boundary routers transmit intra-VPN traffic from sources within the VPN and extra-VPN traffic from sources outside the VPN within separate access network logical connections for intra-VPN and extra-VPN traffic; and a plurality of ingress boundary routers coupled to the one or more egress boundary routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic, **such that denial of service attacks on said access link originating from sources outside the VPN can be prevented**."

According to the Office Action (on page 3), *Liu* discloses a network system that resists denial of service attacks on an access link to a destination host belonging to a virtual private network. Applicant respectfully disagrees with this contention, as *Liu* provides no factual support. *Liu* is instead directed to a system for managing a virtual private network operating over a public data network, which has no provision for resisting denial of service

attacks. The system receives a command specifying an operation on the virtual private network and determines which virtual private network gateways are affected by the command. The system then automatically translates the command into configuration parameters for virtual private network gateways affected by the command; the configuration parameters specifying how the virtual private network gateways handle communications between specific groups of addresses on the public data network. The configuration parameters are then transmitted to the virtual private network gateways affected by the command, so that the virtual private network gateways are configured to implement the command. The system may use the configuration parameters to determine whether the source and destination addresses of a communication between nodes in the public data network belong to the same virtual private network. If the source and destination addresses belong to the same virtual private network, the system ensures that the communication is transmitted securely over the public data network. (col. 3: 1-31) There is no mention or suggestion anywhere in *Liu* of resisting denial of service attacks.

Further, the Office Action asserts that "wherein said one or more egress boundary routers transmit intra-VPN traffic from sources within the VPN and extra-VPN traffic from sources outside the VPN within separate access network logical connections for intra-VPN and extra-VPN traffic" recited by claim 1 is supposedly disclosed by *Liu* at col. 7: 20-45 and Fig. 2. (Office Action, page 3) However, the system of *Liu* processes a packet proceeding from an endstation 112 over a LAN 110 to a routing device 114, which encapsulates the data packet in accordance with the Internet Protocol, forming an outbound IP packet. A VPN gateway determines whether the source and destination addresses of the data packet are both members of the same VPN group. If not, the packet is forwarded to the Internet as ordinary Internet traffic from the site or discarded, and if yes, then the data

packet is processed by compression, encryption, and authentication according to respective algorithms associated with each VPN group, and is then forwarded toward the destination address over the Internet. (col. 7: 8 - col. 8: 10) There is no suggestion or disclosure of "separate access network logical connections for intra-VPN and extra-VPN traffic" as recited by claim 1.

The Office Action correctly acknowledges that the "plurality of ingress boundary routers coupled to the one or more egress boundary routers" as recited by claim 1 is not disclosed by *Liu*. (Office Action, page 3) *Tabata* is applied for supposedly disclosing "a plurality of ingress boundary routers coupled to the one or more egress boundary routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic, **such that denial of service attacks on said access link originating from sources outside the VPN can be prevented**" at paragraphs 0046, 0048, 0084, and 0091. *Tabata*'s system is intended to secure a required bandwidth for end users of an IP VPN, providing interconnection to networks having an MPLS scheme. (par. 0010)

As best understood, the Office Action equates the ingress edge node of edge node 2 with the recited "ingress boundary routers" and the egress edge node with the recited "one or more egress boundary router" of claim 1. (par. 0046) However, these nodes are not shown in Fig. 1, and there is no disclosure that the ingress edge node is coupled to the egress edge node, as would be required by claim 1. The Office Action apparently references *Tabata* (par. 0084) for its discussion of limiting input bandwidth of an in-network packet by acquiring bandwidth information from ingress transfer control information. An in-network packet exceeding a predetermined bandwidth is discarded. In contrast, claim 1 recites "logically partitioning intra-VPN and extra-VPN traffic," which is nowhere suggested or disclosed by *Tabata.* Moreover, *Tabata's* limiting of the input

bandwidth of an in-network packet does not satisfy "a plurality of ingress boundary routers coupled to the one or more egress boundary routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic, **such that denial of service attacks on said access link originating from sources outside the VPN can be prevented**" as recited by claim 1, since the restriction on the bandwidth occurs on **in-network packets** according to predetermined quality control information to perform control such that an in-network packet exceeding the bandwidth based on a contract with a user is not transmitted to the backbone network of *Tabata*. (par. 0026) This deficiency is not cured by any reasonable combination of *Liu* and *Tabata*. Therefore, the rejection of claim 1 should be withdrawn.

Independent claim 9 recites "a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic, **such that denial of service attacks on said access link originating from sources outside the VPN can be prevented**," and independent claim 16 recites "transmitting intra-VPN traffic from said one or more egress boundary routers toward the destination host via the first logical connection, and transmitting extra-VPN traffic from said one or more egress boundary routers toward the destination host via the second logical connection, **such that denial of service attacks on said access link originating from sources outside the VPN can be prevented.**" For reasons similar to those discussed above, the rejections of claims 9 and 16 should also be withdrawn.

The rejection of dependent claims 2-8, 10-15, and 17-20 should be withdrawn for at least the same reasons as their respective independent claims, and these claims are separately patentable on their own merits.

Independent claim 21 recites a "method for resisting denial of service attacks on an access link to a destination host included in a VPN." In its rejection of claim 21, the Office

Action asserts that it would have been obvious to "modify the teachings of Liu such that precedence information is used to partition the traffic," and that the motivation would be to "prevent a bandwidth consumption attack." (Office Action, page 7) However, the system of *Liu* examines packets to determine whether or not they are VPN traffic. Packets determined to be VPN traffic are processed for compression, encryption, and authentication rules according to the packet's VPN group, and packets determined to be non-VPN traffic are either passed through or discarded. (col. 8: 17-39) The system of *Tabata* restricts the bandwidth for **in-network packets** according to predetermined quality control information to perform control such that an in-network packet exceeding the bandwidth based on a contract with a user is not transmitted to the backbone network of *Tabata.* (par. 0026) This is done to "secure a required bandwidth for each end user" in order to **ensure a communication bandwidth available to each end user for quality control**. (pars. 0007 and 0010) Even if the two references were combinable, this type of modification to the system of *Liu* would do no more than ensure a communication bandwidth to each end user for quality control, and would not resist "**denial of service attacks on an access link to a destination host included in a VPN**." This deficiency is not satisfied by any reasonable combination of *Liu* and *Tabata.* Therefore, the rejection of claim 21 should be withdrawn.

Therefore, the present application overcomes the rejections of record and is in condition for allowance. Favorable consideration is respectfully requested. If any unresolved issues remain, it is respectfully requested that the Examiner telephone the undersigned attorney at 703-425-6499 so that such issues may be resolved as expeditiously as possible.

Respectfully Submitted,

DITTHAVONG & CARLSON, P.C.

June 24, 2004
Date

Margo Livesay
Reg. No. 41,946

Phouphanomketh Ditthavong
Reg. No. 44,658

Attorney/Agent for Applicant(s)

10507 Braddock Road
Suite A
Fairfax, VA 22032
Tel. 703-425-6499
Fax. 703-425-8518